REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-9 are currently pending. Claims 1 and 8 have been amended. Claim 9 has been added by the present amendment. The changes and additions to the claims do not add new matter and are supported by the originally filed specification.

In the outstanding Office Action, Claims 1, 2, 6 and 8 were rejected under 35 U.S.C. § 102(b) as anticipated by Mittra (U.S. Patent No. 5,748,736); Claims 3 and 4 were rejected under 35 U.S.C. § 103(a) as unpatentable over Mittra in view of Pearce et al. (U.S. Patent No. 6,804,254, hereinafter "Pearce"); Claim 5 was rejected under 35 U.S.C. § 103(a) as unpatentable over Mittra in view of JP 11239163 A (hereinafter, "JP '163"); and Claim 7 was rejected under 35 U.S.C. § 103(a) as unpatentable over Mittra.

In view of the rejection of Claims 1, 2, 6, and 8 under 35 U.S.C. § 102(b) as anticipated by Mittra, Claim 1 has been amended to recite a communication system including the additional features of an information providing-side network configured to provide connectivity to the information providing unit, to restrict access to the information providing-side network, and to operate under a first security policy restricting access to the information providing-side network based on an authentication determination made from within the information providing-side network, an information transmitting-side network configured to provide connectivity to the information transmitter, to restrict access to the information transmitting-side network, and to operate under a second security policy restricting access to the information transmitting-side network based on an authentication determination made from within the information transmitting-side network. Support for these features can be found in the originally file specification on page 8, lines 9-28 and page 9, lines 17-31. No new matter has been added. Independent Claim 8 has been amended similar to Claim 1.

Briefly recapitulating, amended Claim 1 is directed to a communication system having an information providing unit configured to provide information data, an information providing-side network configured to provide connectivity to the information providing unit, to restrict access to the information providing-side network, and to operate under a first security policy restricting access to the information providing-side network based on an authentication determination made from within the information providing-side network, an information transmitter configured to obtain the information data by transmitting request data for requesting the information data to the information providing unit, and transmit obtained information data to a terminal, an information transmitting-side network configured to provide connectivity to the information transmitter, to restrict access to the information transmitting-side network, and to operate under a second security policy restricting access to the information transmitting-side network based on an authentication determination made from within the information transmitting-side network, and a transfer unit having an interface for each of the information transmitting-side network and the information providing-side network. The transfer unit is configured to connect to each of the networks, determine whether or not transmitting-side data received via the information transmitting-side network is data transmitted from the information transmitter, and whether or not providing-side data received via the information providing-side network is data transmitted from the information providing unit, and transfer the transmitting-side data and the providing-side data based on determination results.

In a non-limiting example, Figure 2 shows the communication system 1 with the information providing unit 10, the information providing-side network 20, the information transmitter 60, the information transmitting-side network 50, and the transfer device 40. In the example of Figure 2, access to the information providing side network 20 is restricted to terminals allowed by the authentication server 21, which operates under a first security policy

restricting access to the information providing-side network based on an authentication determination made from within the information providing-side network (see page 8, lines 9-28). Similarly, access to the information transmitting-side network 50 is restricted to terminals allowed by the authentication server 51, which operates under a second security policy restricting access to the information transmitting-side network based on an authentication determination made from within the information transmitting-side network (see page 9, lines 17-31).

Turning to the applied art, Mittra is directed to a system and method for secure group communications via multicast or broadcast. As shown in Fig. 1, Mittra discloses a hierarchy of multicast/unicast networks that are connected by Trusted Intermediaries (TIs), where a secure multicast message can be transmitted from a high level network such as 112A to a lower level network such as 112B or 112D (see col. 12, lines 30-38). Mittra teaches that to restrict access to a secure multicast message, the message is encrypted and a key can be used by the receiver to unencrypt the message (see col. 7, lines 8-11, and col. 12, lines 55-61).

However, Applicants respectfully submit that Mittra fails to teach or suggest an information providing-side network configured to restrict access to the information providing-side network and an information transmitting-side network configured to restrict access to the information transmitting-side network as required by Claims 1 and 8. Rather, Mittra merely discloses restricting access to individual encrypted messages (see col. 12, lines 55-61) or to individual communication lines (see col. 6, lines 59-60). In either case, Mittra **does not teach or suggest restricting access to the actual networks.**

To further illustrate that only secure data is restricted in Mittra, as opposed to the network recited in Claims 1 and 8, Mittra notes that when no sensitive data is being multicast then it may be acceptable to not change the key as members join and leave (see col. 9, lines 7-12).

Additionally, Mittra fails to disclose an information providing-side network configured to operate under a first security policy restricting access to the information providing-side network based on an authentication determination made from within the information providing-side network, and an information transmitting-side network configured to operate under a second security policy restricting access to the information transmitting-side network based on an authentication determination made from within the information transmitting-side network, as required by amended Claim 1.

Mittra teaches a hierarchy of multicast/unicast networks where a secure multicast message can be transmitted from a high level network such as 112A to a lower level network such as 112B or 112D (see col. 12, lines 30-38). Mittra teaches that to restrict access to a secure multicast message, the message is encrypted and a key can be used by the receiver to unencrypt the message (see col. 7, lines 8-11, and col. 12, lines 55-61). Therefore, the security policy that is taught by Mittra is based on **restricting access to individual messages instead of restricting access to actual networks**.

Further, Mittra does not teach or suggest an information transmitting-side network where an authentication determination is made from within the information transmitting-side network, as required by amended Claim 1. On the contrary, Mittra states that when a Trusted Intermediary (TI) server, which provides encryption keys for a lower level network, authenticates with the Group Security Controller (GSC) or a parent TI server sitting in a higher level network, it receives an access control list to perform authentication of the terminals in the lower level network (see col. 13, lines 30-33). In other words, the authentication of terminals in an information transmitting-side network of Mittra **is made externally to the information-transmitting side network**.

Accordingly, Applicants respectfully submit that independent Claims 1 and 8, and each of the claims depending there from, patentably distinguish over Mittra.

Regarding the rejections of dependent Claims 3, 4, 5, and 7 under 35 U.S.C. § 103(a), Pearce and JP '163 have been considered but fail to remedy the deficiencies of Mittra as discussed above with regards to amended Claim 1. Accordingly, Applicants respectfully submit that a prima facie case of obviousness has not been established and the rejection of dependent Claims 3, 4, 5, and 7 should be withdrawn.

Thus, it is respectfully submitted that independent Claims 1 and 8 (and all associated dependent claims) patentably define over Mittra, Pearce, and JP '163, either alone or in combination.

New dependent Claim 9 is added to vary the scope of the invention. Dependent Claim 9 is directed to the communication system of Claim 2, but further reciting the transfer unit to include an interface for each of the plurality of information providing-side networks. Claim 9 is supported by Fig. 8 of the instant invention. No new matter has been added.

Applicants respectfully submit that new Claim 9 is not anticipated by Mittra for the following reasons. Mittra fails to disclose a plurality of information providing-side networks, where a transfer unit further has an interface for each of the plurality of information providing-side networks. In order to have an interface for each of a plurality of information-providing side networks in addition to an interface for an information transmitting-side network, a transfer unit would have to interface three networks at a minimum. Rather, Mittra teaches a Group Security Controller (GSC) interfacing one network and each Trusted Intermediary (TI) interfacing a maximum of two networks as shown in Figs. 1-3.

Therefore, if either the GSC or TI of Mittra is regarded as the transfer unit, then it is impossible for either of them to have enough interfaces for a plurality of information providing-side networks in addition to an interface for the transmitting-side network.

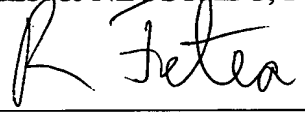
Accordingly, Applicants respectfully submit that new Claim 9 is patentably defined over Mittra. Furthermore, Pearce and JP '163 have been considered but fail to remedy the deficiencies of Mittra as discussed above with regards to Claim 9.

Thus, it is respectfully submitted that dependent Claim 9 patentably defines over Mittra, Pearce, and JP '163, either alone or in combination.

Consequently, in light of the above discussion and in view of the present amendment, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Remus F. Fetea, Ph.D.
Registration No. 59,140

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\SG\270750US\270750US-AM 03-12-07.DOC